JOURNAL OF COMBINATORIAL THEORY (A) 23, 180–186 (1977)

A Construction for Equidistant Permutation Arrays of Index One

S. A. VANSTONE AND P. J. SCHELLENBERG

University of Waterloo, Waterloo, Ontario, Canada

Communicated by the Managing Editors

Received September 29, 1976

An equidistant permutation array (EPA) which we denote by $A(r, \lambda; v)$ is a $v \times r$ array such that every row is a permutation of the integers 1, 2,..., r and such that every pair of distinct rows has precisely λ columns in common. $R(r, \lambda)$ is the maximum v such that there exists an $A(r, \lambda; v)$. In this paper we show that $R(n^2 + n + 2, 1) \geqslant 2n^2 + n$ where n is a prime power.

1. INTRODUCTION

An equidistant permutation array (EPA) is a $v \times r$ array in which every row is a permutation of the integers 1, 2,..., r and every pair of distinct rows has precisely λ columns in common. We denote such an array by $A(r, \lambda; v)$ and call λ the index of the array.

Bolton [2] defines $R(r, \lambda)$ to be the maximum v for which there exists an $A(r, \lambda; v)$. It has been shown by Deza [4] that $R(r, \lambda) \leqslant \max\{\lambda + 2, k^2 + k + 1\}$ where $k = r - \lambda$. In [5] it is shown that $R(r, 1) \leqslant r(r - 3)$ and in [6] that for any integer $r > 2$, $R(2r + 1, 1) \geqslant 2r + 2$. In [7], construction techniques for $A(r, 2; r)$'s, r a prime power, are described.

This paper gives a construction for EPAs which implies $R(n^2 + n + 2, 1) \geqslant 2n^2 + n$ for n a prime power.

A generalized Room square (GRS) is an $r \times r$ array defined on a symbol set V of cardinality v such that every element of V is contained in every row and column of the array precisely once, every cell contains a subset (possibly empty) of V and every pair of distinct elements of V is contained in λ of the cells. Such an array will be denoted $S(r, \lambda; v)$.

An (r, λ) design is a collection B of subsets (called blocks) taken from a finite set V of elements (called varieties) such that every variety is contained in precisely r blocks and every distinct pair of varieties is contained in exactly λ of the blocks. If the cardinality of V is v we denote an (r, λ) design by $D(r, \lambda; v)$. A $D(r, \lambda; v)$ is called a resolvable (r, λ) design ($RD(r, \lambda; v)$) if the blocks of the design can be partitioned into classes (called resolution classes)

such that every variety is contained in precisely one block of each resolution class. A partitioning of the blocks into resolution classes is called a resolution of the design. An $RD(r, \lambda; v)$ is said to be an orthogonal (r, λ) design ($OD(r, \lambda; v)$) if the design has two resolutions R and S, where $R_1, R_2, \ldots, R_r$ and $S_1, S_2, \ldots, S_r$ are the resolution classes of R and S, respectively, such that for all i and j, $1 \leqslant i, j \leqslant r$, R_i and S_j have at most one block in common.

The following result appears in [6].

THEOREM 1.1. *The existence of any one of the following three implies the existences of the other two*:

(1) $A(r, \lambda; v)$;
(2) $S(r, \lambda; v)$;
(3) $OD(r, \lambda; v)$.

We prefer to think of EPAs in terms of GRSs and orthogonal (r, λ) designs. Hence the remainder of the paper will be cast in these terms.

2. PRELIMINARIES

In this section we present certain definitions and results which will be useful in later sections.

A starter S of index λ and order t in a finite additive Abelian group G is a partitioning of the elements of G into an ordered set of subsets, $(B_1, B_2, \ldots, B_t)$, such that if $D_g = \{(a, b): a, b \in B_i \text{ for some } i \text{ and } a - b = g\}$ then $| D_g | = \lambda$ (a constant) for all $g \in G \backslash \{0\}$. Define $B_i + g = \{b + g: b \in B_i\}$. It can be verified that the collection of blocks $B_i + g$, for all $i \in \{1, 2, \ldots, t\}$ and all $g \in G$, forms a resolvable $(| G |, \lambda)$ design on $| G |$ elements.

As an example, the blocks $\{1, 2, 4\}, \{0\}, \{3\}, \{5\}, \{6\}$ form a starter of index 1 in the integers modulo 7 and can be used to generate a (7, 1) design on seven elements.

An adder A for a starter S of index λ and order t is an ordered set $(a_1, a_2, \ldots, a_t)$ of distinct elements of G such that

$$\bigcup_{i=1}^{t} B_i + a_i = G.$$

THEOREM 2.1. *If there exists a starter S of index λ in a finite Abelian group G and an adder A for S then there exists an $S(r, \lambda; r)$ where $r = | G |$.*

Proof. Label the rows and columns of an $r \times r$ array with the elements of G. For any $g, h \in G$, and for any $i \in \{1, 2, \ldots, t\}$, place the block $B_i + g$ in cell (g, h) iff $h - g = a_i$. We now show that this array is a GRS.

The blocks in row zero are $B_1, B_2, \ldots, B_t$, the blocks of the starter S, and by definition are a partition of the elements of G. The blocks in row g are

$B_1 + g, B_2 + g, \ldots, B_t + g$ and it is easy to show that these blocks partition the elements of G.

The blocks in column zero are $B_1 + a_1, B_2 + a_2, \ldots, B_t + a_t$. From the definition of an adder it follows that these blocks partition G. Consider the cells of column h. Cell (g, h) contains a block iff $h - g = -a_i$ for some a_i of A. This implies $g = a_i + h$ and the block in this cell is $B_i + a_i + h = (B_i + a_i) + h$. Thus the blocks in column h are $(B_1 + a_1) + h, (B_2 + a_2) + h, \ldots, (B_t + a_t) + h$ and it is easy to see that these blocks partition G. Thus every variety of G is contained in precisely one cell of each line of the array.

Since the blocks $B_i + g$, for all $i \in \{1, 2, \ldots, t\}$ and all $g \in G$, constitute an (r, λ) design every variety is contained in precisely λ cells of the array. Thus the array is an $S(r, \lambda; r)$ where $|G| = r$. ∎

We also require a graph theoretic result. The notation and terminology used in this discussion is that of Bondy and Murty [3].

Consider the complete directed graph K_n^* on n vertices. If $v_1, v_2, \ldots, v_n$ are the vertices of K_n^* then for all ordered pairs (v_i, v_j), $i \neq j$, there is precisely one arc from v_i to v_j. A directed cycle in K_n^* is a finite nonnull sequence

$$(v_{i_0}, a_{i_1}, v_{i_1}, a_{i_2}, v_{i_2}, \ldots, v_{i_{k-1}}, a_{i_k}, v_{i_0}),$$

where $v_{i_0}, v_{i_1}, \ldots, v_{i_{k-1}}$ represent distinct vertices of K_n^* and $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ represent distinct arcs of K_n^* such that arc a_{i_r} joins vertex $v_{i_{r-1}}$ to v_{i_r}, for $r = 1, 2, \ldots, k-1$, and arc a_{i_k} joins $v_{i_{k-1}}$ to v_{i_0}. This directed cycle is often represented simply by its vertex sequence $(v_{i_0}, v_{i_1}, \ldots, v_{i_{k-1}}, v_{i_0})$.

The following result is established by Bermond and Faber [1].

THEOREM 2.2. *For any positive integer n the arcs of K_{n+1}^* can be partitioned into directed cycles of length n.*

For the sake of completeness we briefly describe the construction of Bermond and Faber.

To the ring of integers modulo n, $R = \mathbb{Z}n$, adjoin an infinite element, ∞, such that for any $g \in R$, $g + \infty = \infty + g = \infty$. Label the vertices of K_{n+1}^* with the elements of $R \cup \{\infty\}$. For $a, b \in R$, label the arc joining vertex a to vertex b by $(a - b)$. For n even, consider the cycle

$$C = \left(\infty, 0, n-1, 1, n-2, 2, \ldots, n - \left(\frac{n}{2} - 1\right), \frac{n}{2} - 1, \infty\right).$$

For $g \in R$, let $C + g$ be the cycle of length n

$$C + g = \left(\infty, 0 + g, (n-1) + g, 1 + g, (n-2) + g, 2 + g, \ldots, \left(n - \left(\frac{n}{2} - 1\right)\right) + g, \left(\frac{n}{2} - 1\right) + g, \infty\right).$$

Using the fact that no two arcs in the cycle C have the same finite label, it can be shown that the cycles $C + g$, $g \in R$, are arc disjoint. Furthermore, none of them has the label 1. The decomposition into cycles of length n is completed by adjoining the cycle

$$D = (0, 1, 2, \ldots, n - 1, 0).$$

For n odd, let

$$C = \left(\infty, 0, n - 1, 1, n - 2, 2, \ldots, \left[\frac{n}{4}\right] - 1, \left[\frac{3n}{4}\right] + 1, \left[\frac{n}{4}\right], \left[\frac{3n}{4}\right] - 1,\right.$$
$$\left.\left[\frac{n}{4}\right] - 1, \ldots, \left[\frac{n}{2}\right] + 2, \left[\frac{n}{2}\right] - 2, \left[\frac{n}{2}\right] + 1, \left[\frac{n}{2}\right] - 1, \left[\frac{n}{2}\right], \infty\right),$$

where $[x]$ represents the integer part of x. Again it can be shown that the cycles $C + g$, $g \in R$ are arc disjoint. None of the arcs in C have the label $[n/2] + 1 = a$. The decomposition is completed by adjoining the cycle

$$D = (0, a, 2a, 3a, \ldots, (n - 1)a, 0).$$

3. The Construction

THEOREM 3.1. *If there exists a starter S of index 1 and order t in a finite Abelian group G such that S contains k blocks of cardinality one, and if there exists an adder A for S then there exists*:

(1) *an* $S(|G|, 1; |G|)$ *if* $k = 0$;

(2) *an* $S(|G|, 1; |G| + 1)$ *if* $k = 1$;

(3) *an* $S(|G| + 1, 1; |G| + k - 1)$ *if* $k \geqslant 2$.

Proof. (1) is just a restatement of Theorem 2.1. In (2) let B_1 be the block of size 1 in S. Form a new block $B^* = B_1 \cup \{\infty\}$ where $\infty + g = \infty$ for all $g \in G$. Applying the construction of Theorem 2.1 gives the desired result.

Now consider (3). Let $B_1, B_2, \ldots, B_k$ be the blocks of size one in S. Form new blocks $B_1^*, B_2^*, \ldots, B_{k-1}^*$ such that

$$B_i^* = B_i \cup \{\infty_i\}, \qquad 1 \leqslant i \leqslant k - 1,$$

where $\infty_1, \infty_2, \ldots, \infty_{k-1}$ are distinct and different from the elements of G and $\infty_i + g = \infty_i$ for all $g \in G$ and $1 \leqslant i \leqslant k - 1$.

Replace the blocks $B_1, B_2, \ldots, B_{k-1}$ in S with $B_1^*, B_2^*, \ldots, B_{k-1}^*$. If a_i is the adder element corresponding to B_i then a_i corresponds to B_i^*, $1 \leqslant i \leqslant k - 1$. Applying the construction in Theorem 2.1 to these blocks produces an array A which is $|G| \times |G|$, having all of the properties of a GRS except that the varieties ∞_i, ∞_j $(i \neq j)$ never occur together in the same cell.

Since $|B_k| = 1$, A also has the property that there exist $|G|$ cells, denoted T, one from each row and column of A such that each contains a subset of size one and the union of these is G. Construct a new array A^* from A by adjoining a row and column, each labeled *, to A. In cell (*, *) of A^* place $\{\infty_1, \infty_2, \ldots, \infty_{k-1}\}$. If (i,j) is a cell of T and g is the entry in (i,j) place g in cells $(*,j)$ and $(i,*)$ of A^* and remove g from cell (i,j). Do this for all cells of T. Since the cells of T contain all elements of G, row * and column * of A contain each of the elements from $G \cup \{\infty_1, \infty_2, \ldots, \infty_{k-1}\}$ precisely once. The pairs $\{\infty_i, \infty_j\}$ $(i \neq j)$ are contained in cell (*, *) and all other pairs are contained in precisely one cell of the subarray A. Thus A^* is an $S(|G| + 1, 1; |G| + k - 1)$ and the proof is complete. ∎

As an example consider the following starter S and adder A in the integers modulo 7:

S: $B_1 = \{0\}$, $B_2 = \{3\}$, $B_3 = \{5\}$, $B_4 = \{6\}$, $B_5 = \{1, 2, 4\}$;
A: (3, 4, 1, 6, 0).

124			3^{∞}_2	0^{∞}_1		5^{∞}_3	6
6^{∞}_3	235			4^{∞}_2	1^{∞}_1		0
	0^{∞}_3	346			5^{∞}_2	2^{∞}_1	1
3^{∞}_1		1^{∞}_3	045			6^{∞}_2	2
0^{∞}_2	4^{∞}_1		2^{∞}_3	156			3
	1^{∞}_2	5^{∞}_1		3^{∞}_3	026		4
		2^{∞}_2	6^{∞}_1		4^{∞}_3	013	5
5	6	0	1	2	3	4	$^{\infty}1\ ^{\infty}2$ $^{\infty}3$

S(8,1;10)

16485273
12758634
42316875
15342786
82645317
28375641
53841672
45671238
56712348
23456718

A(8,1;10)

Using Theorem 1.1, this $S(8, 1; 10)$ implies the $A(8, 1; 10)$ shown above.

4. A Family of EPAs of Index 1

In this section we produce an infinite family of starters and corresponding adders which can be used in Theorem 3.1.

A well-known result of Singer [8] says that in the ring, R, of integers modulo $n^2 + n + 1$, where n is a prime or a prime power, there exists a set B_0 of $n + 1$ elements such that every nonzero element of R occurs as a difference of two elements of B_0 precisely once. Let the elements of $R\backslash B_0$ be partitioned into subsets of cardinality one labeled $B_1, B_2, \ldots, B_{n^2}$. Clearly $S = (B_0, B_1, \ldots, B_{n^2})$ is a starter of index 1 in R. In the following theorem we show there is an adder for S.

THEOREM 4.1. *There exists an adder A for S in $R = \mathbb{Z}_{n^2+n+1}$ where n is a prime or a prime power.*

Proof. For $i \in R$, let $C_i = B_0 + i$. Suppose $g_0 \in C_0$. g_0 is contained in $n + 1$ of the blocks $C_0, C_1, \ldots, C_{n^2+n}$. Denote these as $E_0 = C_0, E_1, E_2, \ldots, E_n$. Since S is of index one

$$\bigcup_{i=1}^{n} E_i\backslash\{g_0\} = R\backslash C_0 .$$

Now consider the complete directed graph K^*_{n+1} with the vertices labeled with elements of C_0. By Theorem 2.2, the arcs of K^*_{n+1} can be partitioned into directed cycles of length n. For any $\{i, j\} \subseteq C_0$, label arc (i, j) of K^*_{n+1} with $(i - j) \in R$. Since the differences between elements of C_0 contain every element of $R\backslash\{0\}$ precisely once, every arc of K^*_{n+1} has a distinct label from $R\backslash\{0\}$. In the partitioning of K^*_{n+1}, for any $g \in C_0\backslash\{g_0\}$, there is precisely one directed cycle of length n not incident with vertex g.

For $t = 1, 2, \ldots, n$, let $E_t = \{e_0 = g_0, e_1, \ldots, e_n\} = C_0 + i$, $i \in R$. If the elements of C_0 are $g_0, g_1, g_2, \ldots, g_n$ then there is a directed cycle C in K^*_{n+1} of length n which does not pass through $e_0 - i \in C_0$ and which we denote $(g_1', g_2', g_3', \ldots, g_n', g_1')$. If $g_j' - g_{j+1}' = d$ then $g_{j+1}' + d = g_j'$ and thus $g_{j+1}' + i + d = g_j' + i$. Let d be the adder element for the block of cardinality one $\{g_{j+1}' + i\}$. Similarly for each j, $1 \leqslant j \leqslant n$, an adder element can be determined for $\{g_j' + i\}$. Since $e_0 - i \neq e_0 - j$ unless $i = j$, each E_t, $1 \leqslant t \leqslant n$, can be associated with a distinct directed n cycle in the decomposition of K^*_{n+1}. Also, since every nonzero element of R occurs as a difference between vertex labels precisely once, all of the adder elements must be distinct and nonzero. Because of the directed cycles the elements of $E_t\backslash\{e_0\}$ are permuted by the corresponding adder elements. ∎

THEOREM 4.2. *If n is a prime or prime power then there exists an $S(n^2 + n + 2, 1; 2n^2 + n)$.*

Proof. Using the starter S of this section in Theorem 3.1, we have $k = n^2$. Since S has an adder, Theorem 3.1 yields the desired result and the proof is complete. ∎

By Theorem 1.1 when n is a prime or a prime power there exists an $A(n^2 + n + 2, 1; 2n^2 + n)$ and thus $R(n^2 + n + 2, 1) \geqslant 2n^2 + n$.

REFERENCES

1. J. C. BERMOND AND V. FABER, Decomposition of the complete directed graph into k-circuits, *J. Combinatorial Theory Ser. B.*, to appear.
2. D. W. BOLTON, Problem, *in* "Combinatorics" (D. Y. A. Welsh and D. R. Woodall, Eds.), pp. 351–352, Math. Inst., Oxford, 1972.
3. J. A. BONDY AND U. S. R. MURTY, "Graph Theory with Applications," Basingstore Macmillan, London, 1976.
4. M. DEZA, Matrices dont deux lignes quelconques coincident dans un nombre donne de positions communes, *J. Combinatorial Theory Ser. A*, to appear.
5. M. DEZA, R. C. MULLIN, AND S. A. VANSTONE, *Orthogonal systems*, to appear.
6. M. DEZA, R. C. MULLIN, AND S. A. VANSTONE, Room squares and equidistant permutation arrays, *Ars Combinatoria*, to appear.
7. F. HOFFMAN, P. J. SCHELLENBERG, AND S. A. VANSTONE, A Starter-adder approach to equidistant permutation arrays and generalized Room squares, *Ars Combinatoria* **1** (1976), 307–320.
8. J. SINGER, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.